A Collaborative Intrusion Detection Based on K-means and Projective Adaptive Resonance Theory

Yi Yi Aung
yiyiaung123@gmail.com
University of Computer Studies, Mandalay, UCSM

Myat Myat Min
myatiimin@gmail.com
University of Computer Studies, Mandalay, UCSM

Since the start of the 21st century, computer networks have been through an exponential growth in terms of the network capacity, the number of the users and the type of tasks that are performed over the network. With the improving advanced technology of portable devices such as smart phones, tablet, smart devices, other computing devices, the number of network users are increasing more and more. Hence, security on network is very important for all net consumers. Intrusion detection is the process of defending intrusions. The action of entering to a system without permission is called intrusion. An intrusion detection system (IDS) can detect all incoming and out coming intrusion to the system. IDS can inspect all possible violations of a security guideline by monitoring system activities. Since IDS are fundamental part of security boundary, it can afford the ability to identify security holes in a ystem. There are many current methods used in intrusion detection. This paper analyzes the comparison between hybrid data mining methods and single method. The purpose of the system is to show that using hybrid data mining methods can reduce time complexity of the system than single method. This model was verified using KDD'99 data set. Experimental results clearly show that hybrid methods using K-means and Projective Adaptive Resonance Theory can significantly reduce model training time of the system and also it maintains the accuracy of detections.